Risk Management Approaches to Protection

July 12, 2005

Martha Marsh
President & CEO
Stanford Hospital and Clinics

Tom Noonan
Chairman, President & CEO
Internet Security Systems, Inc.

Agenda

- NIAC Question
- Timeline
- Study Group Approach
- Study Group Initial Findings
- Study Group Thoughts About Potential Recommendations
- Next Steps
- Discussion

NIAC Question

- "Can private sector experience with risk management and prioritization provide meaningful guidance to the President for risk management for national critical infrastructure planning and programs by the government?"
- NIAC cited private sector experience with risk management

  Experience includes managing IT and physical risk
  - Financial/commercial risk
  - Magnitude & duration of consequences
  - Customer & public impact by and acceptance of the consequences
  - Event experience, including:
    - Weather
    - Supply disruptions
    - Network disruptions
    - Commodity volatility

Timeline

- Initiate Working Group (October '04 NIAC)
  - Identify and recruit stakeholders
  - Define scope and timeline; resources and allocation
- Data Aggregation and Assessment (January '05 NIAC)
  - Aggregate raw risk management data
  - Assess state of risk management methods
- Deliverable Development (July '05 NIAC)
  - Report on deliverable development progress
  - Present initial study group thoughts on potential recommendations for review and comment
- Report Delivery (October '05 NIAC)
  - Present final deliverable

Study Group Approach

- Study Group initiated efforts to:
  - Aggregate and assess existing public and private sector risk management methodologies, practices, and decision models
  - Identify risk management commonalities and differences at both the strategic and operational levels
  - Identify trends in private sector risk management maturity; benchmark these trends against public sector risk management
  - Provide thoughts about potential recommendations of value on behalf of NIAC that will strengthen federal risk management practices

Study Group Approach (cont.)

- Stakeholder incorporation:
  - Addressed risk management across multiple industries represented by NIAC (finance, technology, electric, health, etc)
  - Identified and enlisted external stakeholders from
    - Academia (e.g. Stanford, Dartmouth, Maryland)
    - Industry associations (NACD, NERC, IIA)
    - Government agencies (DHS and DoD DCMA)
  - Conducted interviews, captured feedback, and included working papers in the work group document library
  - Addressed risk management at tactical, operational and strategic levels

Study Group Approach (cont.)

- Completed data collection and analysis:
  - Developed document library with contributions from multiple sectors, covering strategic and operational risk management
  - Included input from associations, academia, government and industry. Library covered private and public sectors
  - Validated input with risk management stakeholders (e.g. associations), industry representatives (e.g. NERC); substantial contributions from academia on more technical aspects of risk management (e.g., risk quantification)

Study Group Initial Findings

- Risk management is enhanced when predicated upon past performance
  - Significant actuarial, and historical, risk management data improves the ability of organizations to assess and manage risk
  - Some areas of risk lend themselves well to this type of analysis, others do not
    - Discussion on specific attributes of mature/immature (effective/ineffective) models

Study Group Initial Findings (cont.)

- Across all industries and sectors are examples of effective and ineffective risk management
- Contrasting risk acceptance levels between public and private sectors
- Effective risk management
  - Highly actuarialized data; mature understanding of failure mechanisms and failure indicators
  - Effective use of data; Actionable information; Proximity between actuaries, indicators, and decision-makers
  - Competition and consumer choice encourage effective risk management
  - Understanding and appreciation of legal precedent provides foundation for qualitative nature of risk management
  - Risk management culture across organization; single, senior accountable individual
  - Aligned incentive factors
  - Mechanisms to reduce human error (e.g., training, technology, procedures, etc.)
  - Insurance mechanisms to improve risk tolerance
  - Substantiated business case for risk management investments

Study Group Thoughts on Potential Findings (cont.)

- Immature (ineffective) risk management
  - Lack of highly actuarialized data; immature understanding of failure mechanisms and failure indicators
  - Ineffective use of data, or data that is not translated into actionable intelligence; lack of proximity between data points and decision-makers
  - Few (or no) competitive forces driving more advanced risk management
  - Limited (or no) understanding of legal precedent compelling risk management outcomes
  - Limited (or no) organizational risk management culture; lack of single, senior, accountable risk management leadership Mis-aligned incentive factors
  - Mis-aligned incentive factors
  - Lack of mechanisms to reduce human error
  - Lack of insurance mechanisms to improve risk tolerance
  - Unsubstantiated or poorly developed business case for risk management investments

Study Group Thoughts About Potential Recommendations

- Continue to engage the resources of the government to:
  - Educate both public and private sector on risk management
  - Outline an approach for national risk management
  - Develop and implement a risk management framework
- Continue to promote and expand the public-private sector risk management partnership
- Create a risk management infrastructure, mechanisms and methodologies
  - Develop mechanisms to identify, acquire, collect, and analyze risk management data; create actionable intelligence
  - Develop and implement risk management data warehouse
  - Identify and implement incentive mechanisms to maximize robustness of risk management data warehouse and maximize stakeholder contributions

Study Group Thoughts on Potential Recommendations (cont.)

- Establish risk management leadership function within departments, bureaus or agencies
  - Single, senior focal point for organizational risk management decision-making (similar to corporate Chief Risk Officer role)
- Analyze and prioritize threats to the critical infrastructure
  - Use mechanisms and infrastructure to develop mitigation strategy
  - Establish risk management priorities for the organization
  - Makes risk management recommendations to organizational lead
- Establish independent risk management oversight function for departments, bureaus or agencies
  - Establish a body responsible for organizational risk management oversight (functions similar to corporate Board of Directors)
  - Establish risk management metrics, including incentives and penalties
  - Establish, at the senior-most level, a risk management culture

Next Steps

- Advance "Study Group" initial findings and thoughts on potential recommendations to "Working Group"
- Working Group coordinate with NIAC leadership to gain consensus on findings and recommendations
- Working Group to align written deliverable to final findings and recommendations and circulate prior to October NIAC meeting
- Position Working Group recommendations to be adopted

Discussion

- Questions?